斗象科技
TOPHANT

2024-06

2024
HW 必修高危漏洞集合

版本：v2.0

斗象科技-漏洞情报中心

Email:service@tophant.com

Tel:400-156-9866

让安全无法撼动

目录 CONTENTS

一、 前言

高危风险漏洞一直是企业网络安全防护的薄弱点，也成为 HW 攻防演练期间红队的重要突破口；每年 HW 期间爆发了大量的高危风险漏洞成为红队突破网络边界防护的一把利器，很多企业因为这些高危漏洞而导致整个防御体系被突破、甚至靶标失守而遗憾出局。

HW 攻防演练在即，斗象情报中心依托漏洞盒子的海量漏洞数据、情报星球社区的一手漏洞情报资源以及 Freebuf 安全门户的安全咨询进行分析整合，输出 HW 必修高危漏洞手册，意在帮助企业在 HW 攻防演练的前期进行自我风险排查，降低因高危漏洞而“城池失守”的风险。

本次报告整合了自 2023 年 12 月份至 2024 年 2 月份在攻防演练被红队利用最频繁且对企业危害较高的漏洞，包含了详细的漏洞基础信息、检测规则和修复方案，企业可根据自身资产信息进行针对性的排查、配置封堵策略和漏洞修复相关工作。

《2024HW 必修高危漏洞集合》预计将发布三期

第一期《2024HW 必修高危漏洞集合_1.0》收录 2024 年 3 月-2024 年 5 月

第二期《2024HW 必修高危漏洞集合_2.0》收录 2023 年 12 月-2024 年 2 月

第三期《2024HW 必修高危漏洞集合_3.0》收录 2023 年 8 月-2023 年 11 月

斗象智能安全 PRS 已支持详细检测规则，如需要协助请联系：400-156-9866

2024HW 必修高危漏洞集合持续更新中，请持续关注。

二、 漏洞汇总数据

本文档为斗象发布的《2024HW 必修高危漏洞集合_2.0》对自 2023 年 12 月至 2024 年 2 月份在攻防演练过程红队利用率比较高的漏洞进行总结汇总，具体的数据如下所示：

- 命令执行漏洞

  漏洞数量：5 个

  涉及厂商：万户软件、亿赛通、北京派网软件有限公司、PHP、致远

- 文件上传

  漏洞数量：10 个

  涉及厂商：用友、奇安信、通达、宏景、泛微、金蝶

- 不安全的反序列化

  漏洞数量：2 个

  涉及厂商：用友

- 其他

  漏洞数量：3

  漏洞类型：远程代码执行，SQL 注入

  涉及厂商：Atlassian、致远、泛微

以下为本次高危漏洞自查列表：

漏洞名称	漏洞类型	所属厂商	影响版本
万户 OA RhinoScriptEngineService 命令执行漏洞	命令执行漏洞	万户软件	万户 ezOFFICE 协同管理平台
亿赛通-数据泄露防护(DLP)多个接口 命令执行漏洞	命令执行漏洞	亿赛通	亿赛通电子文档安全管理系统
Panalog 日志审计系统 libres_syn_delete.php	命令执行漏洞	北京派网软件有限公司	Panalog

命令执行漏洞			
PHP8.1.0-dev 后门远程命令执行漏洞	命令执行漏洞	PHP	PHP 8.1.0-dev
致远 OA M1Server userTokenService 远程命令执行漏洞	命令执行漏洞	致远	致远 OA M1Server
用友 U8-OA doUpload.jsp 任意文件上传漏洞	任意文件上传	用友	用友 U8-协同工作系统
用友_移动管理系统 mobsm_common_upload 任意文件上传漏洞	任意文件上传	用友	用友 移动管理系统
用友 GRP-U8 SmartUpload01 文件上传漏洞	任意文件上传	用友	用友 GRP-U8
奇安信天擎 rptsvr 任意文件上传	任意文件上传	奇安信	奇安信 天擎管理中心 <=V6.7.0.4130
通达 OA privateUpload 任意文件上传漏洞	任意文件上传	通达	通达 OA 2011
宏景 eHR OfficeServer.jsp 任意文件上传漏洞	任意文件上传	宏景	宏景 eHR
泛微 E-Office Init.php 任意文件上传漏洞	任意文件上传	泛微	泛微 E-Office
泛微 OA E-mobile lang2sql 任意文件上传漏洞	任意文件上传	泛微	泛微 OA E-mobile
用友 GRP-U8 /servlet/FileUpload 文	任意文件上传	用友	用友 GRP-U8R10

件上传漏洞			
金蝶 EAS /easportal/tools/appUtil.jsp 任意文件上传/下载漏洞	任意文件上传/下载	金蝶	金蝶 EAS
用友 NC XbrlPersistenceServlet 反序列化漏洞	不安全的反序列化	用友	用友 NC
用友 NC DownloadServlet 反序列化漏洞	不安全的反序列化	用友	用友 NC
Atlassian Confluence 远程代码执行漏洞	远程代码执行漏洞	Atlassian	Confluence Data Center and Server 8.0.x Confluence Data Center and Server 8.1.x Confluence Data Center and Server 8.2.x Confluence Data Center and Server 8.3.x Confluence Data Center and Server 8.4.x
致远 OA syncConfigManager 方法存在远程代码执行漏洞	远程代码执行漏洞	致远	致远 OA
泛微 E-Mobile 6.0 Client.do SQL 注入漏洞	SQL 注入漏洞	泛微	泛微 E-Mobile 6.0

三、 自查高危详情

3.1 万户 OA RhinoScriptEngineService 命令执行漏洞

1) 漏洞描述

万户 ezOFFICE 协同管理平台涵盖门户自定义平台、信息知识平台管理、系统管理平台功能，它以工作流引擎为底层服务，以通讯沟通平台为交流手段，以门户自定义平台为信息推送显示平台，为用户提供集成的协同工作环境。

万户 ezOFFICE 协同管理平台 RhinoScriptEngineService 接口存在命令执行漏洞，该漏洞可能导致攻击者获取系统权限、执行任意命令，严重威胁系统的机密性和完整性。

2) 披露时间

2024 年 2 月 27 日

3) 影响版本

万户 ezOFFICE 协同管理平台

4) 检测规则

检测流量中是否存在以下路径：/defaultroot/services/./../RhinoScriptEngineService

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.whir.net

VIP 平台链接：https://vip.vulbox.com/detail/1762315258485149696?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNCVCOCU4NyVFNiU4OCVCN09BJTIwUmhpbm9TY3JpcHRFbmdpbmVTZXJ2aWNlJTIwJUU1JTkxJUJEJUU0JUJCJUE

0JUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.2 亿赛通-数据泄露防护(DLP)多个接口 命令执行漏洞

1) 漏洞描述

亿赛通-数据泄露防护是一款专门防止您的私人数据资产在分享、存储过程中，被他人非法窃取或使用的安全产品。

亿赛通-数据泄露防护(DLP)多个接口存在远程命令执行漏洞，攻击者可以通过该漏洞远程执行代码，控制服务器。

2) 爆发时间

2024 年 2 月 19 日

3) 影响版本

亿赛通电子文档安全管理系统

4) 检测规则

检测流量中是否存对以下接口的访问：

FileCountService

ExamCDGDocService1

EmailAuditService

docRenewApp

DecryptionApp

DecryptApplicationService1

DecryPermissApp

CreateDocService1

clientMessage

ClientLoginWeb

CheckClientServelt

CDGRenewApplication

CDGAuthoriseTempletService1

AutoSignService1

MailMessageLogServices

SystemService

MailApp

GetValidateServerService

GetValidateAuthCodeService

GetUserSafetyPolicyService

GetUsecPolicyService

formType

OutgoingRestoreApp

OfflineApplicationService2

OfflineApplicationService1

offlineApp

ODMSubmitApplyService

UninstallApplicationService1

SecureUsbConnection

outgoingServlet

permissionApp

PrintAuditService

PrintLimitApp

SetEstAlertLogService

UpdateClientStatus

UpdatePasswordService

UpgradeService1

UpgradeService2

UploadFileListServiceForClient

UserLoginOutService1

FileLog2Service

TerminalLogService

GetValidateLoginUserService

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.esafenet.com

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、在输出时对敏感字符进行编码保护，比如 HTML 编码，防止恶意代码直接输出执行。

2、强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。

VIP 平台链接：https://vip.vulbox.com/detail/1759457503785127936?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNCVCQSVCRiVFOCVCNSU5QiVFOSU4MCU5QS0lRTYlOTUlQjAlRTYlOEQlQUUlRTYlQjMlODQlRTklOUMlQjIlRTklOTglQjIlRTYlOEElQTQoRExQKSVFNSVBNCU5QSVFNCVCOCVBQSVFNiU4RSVBNSVFNSU4RiVBMyUyMCVFNSU5MSVCRCVFNCVCQiVBNCVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.3 Panalog 日志审计系统 libres_syn_delete.php 命令执行漏洞

1) 漏洞描述

Panabit Panalog 是一款智能应用网关，致力于提高网络经营中必须的应用可视、成本调优、服务优化、行为管理和审计能力，为用户提供高效、稳定、开放的应用层网络通信平台、产品和服务。

Panalog 日志审计系统 libres_syn_delete.php 接口处存在远程命令执行漏洞，攻击者可以通过该漏洞执行任意命令，接管服务器权限。

2) 爆发时间

2024 年 2 月 18 日

3) 影响版本

Panalog

4) 检测规则

检测流量中是否存在以下路径：

//content-apply/libres

并且请求正文中，是否有“host”参数

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

下载地址：https://www.panabit.com/product-LOG

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、验证用户输入的所有数据，并确保它们符合预期的格式和类型。对输入的数据进行过滤和清理，以防止恶意代码注入。

2、实施严格的访问控制策略，确保只有授权用户能够访问敏感数据和系统资源。

VIP 平台链接 https://vip.vulbox.com/detail/1759038674458251264?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMlBhbmFsb2clMjAlRTYlOTclQTUlRTUlQkYlOTclRTUlQUUlQTElRTglQUUlQTElRTclQjMlQkIlRTclQkIlOUYlMjBsaWJyZXNfc3luX2RlbGV0ZS5waHAlMjAlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.4 PHP8.1.0-dev 后门远程命令执行漏洞

1) 漏洞描述

PHP 版本 8.1.0-dev 于 2021 年 3 月 28 日发布了带有后门的版本，但该后门很快被发现并删除。如果此版本的 PHP 在服务器上运行，攻击者可以通过发送 User-Agentt 标头来执行任意代码。

发现问题后恢复了原代码，但随后又被篡改了第二次。该漏洞将在任何运行受感染版本的 PHP 的网站中创建一个后门，使黑客能够在该网站上执行远程代码执行。

2) 爆发时间

2024 年 1 月 26 日

3) 影响版本

PHP 8.1.0-dev

4) 检测规则

检测请求头中是否存在以下参数：

User-Agentt: zerodiumvar_dump

User-Agentt: zerodiumsystem

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

将 PHP 更新至 8.2.0 及以上版本

VIP 平台链接：https://vip.vulbox.com/detail/1750789095069716480?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMlBIUDguMS4wLWRldiVFNSU5MCU4RSVFOSU5NyVBOCVFOCVCRiU5QyVFNyVBOCU4QiVFNSU5MSVCRCVFNCVCQiVBNCVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNiVCNCU5RSU

yMiU3RA==&origin=intellList

3.5 致远 OA M1Server userTokenService 远程命令执行漏洞

1) 漏洞描述

致远 OA M1Server 是一款企业级办公自动化系统，旨在为企业提供全面的协同办公解决方案。它基于 Web 技术构建，支持多种操作系统和浏览器，具有高度的可扩展性和可定制性。

致远 OA M1Server userTokenService 接口存在远程命令执行漏洞，攻击者可以通过该漏洞获取服务器控制权限，导致服务器失陷。

2) 爆发时间

2024 年 1 月 31 日

3) 影响版本

致远 OA M1Server

4) 检测规则

检测流量中是否存在以下路径：

/esn_mobile_pns/service/userTokenService

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.seeyon.com

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、在输出时对敏感字符进行编码保护，比如 HTML 编码，防止恶意代码直接输出执行。

2、强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。

VIP 平台链接：https://vip.vulbox.com/detail/1752626857452376064?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOCU4NyVCNCVFOCVCRiU5Q09BJTIwTTFTZXJ2ZXIlMjB1c2VyVG9rZW5TZXJ2aWNlJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU1JTkxJUJEJUU0JUJCJUE0JUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJTdEJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.6 用友 U8-OA doUpload.jsp 任意文件上传漏洞

1) 漏洞描述

用友 U8-OA 协同工作系统遵循 J2EE 架构,以 JSP 和 JAVA BEAN 技术作为主要的系统实现手段,开发出了工作流、文档、消息提醒和插件接口。

用友 U8-OA 协同工作系统 doUpload.jsp 接口存在任意文件上传漏洞，未授权的攻击者可以通过该漏洞上传恶意文件，从而控制服务器。

2) 爆发时间

2024 年 2 月 26 日

3) 影响版本

用友 U8-协同工作系统

4) 检测规则

检测流量中是否存在以下路径：

/yyoa/portal/tools/doUpload.jsp

同时检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.yonyou.com VIP 平台链接：https://vip.vulbox.com/detail/1761949576232833024?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QlU4LU9BJTIwZG9VcGxvYWQuanNwJTIwJUU0JUJCJUJCJUU2JTg0JThGJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJUI0JTlFJTIyJTdE&origin=intellList

3.7 用友_移动管理系统 mobsm_common_upload 任意文件上传漏洞

1) 漏洞描述

用友移动系统管理是用友公司推出的一款移动办公解决方案，旨在帮助企业实现移动办公、提高管理效率和员工工作 灵活性 Q。它提供了一系列功能和工具，方便用户在移动设备上管理和处理企业的系统和业务。

用友移动管理系统/mobsm/common/upload 等接口存在任意文件上传漏洞，未经授权攻击者通过漏洞上传任意文件，最终可以获取服务器权限。

2) 爆发时间

2024 年 2 月 22 日

3) 影响版本

用友 移动管理系统

4) 检测规则

检测流量中是否存在以下路径：

/mobsm/common/upload?category

同时检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.yonyou.com

若无法进行升级的情况下，请使用该产品的用户进行如下操作关闭互联网暴露面或设置接口访问权限

VIP 平台链接：https://vip.vulbox.com/detail/1760504220974452736?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QiUyMCVFNyVBNyVCQiVFNSU4QSVBOCVFNyVBRSVBMSVFNyU5MCU4NiVFNyVCMyVCQiVFNyVCQiU5RiUyMG1vYnNtX2NvbW1vbl91cGxvYWQlMjAlRTQlQkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.8 用友 GRP-U8 SmartUpload01 文件上传漏洞

1) 漏洞描述

用友 GRP-U8 行政事业内控管理软件是一款专门针对行政事业单位开发的内部控制管理系统，旨在提高内部控制的效率和准确性。该软件/u8qx/SmartUpload01.jsp 接口存在文件上传漏洞，未经授权的攻击者可通过此漏洞上传恶意后门文件，从而获取服务器权限。

2) 爆发时间

2024 年 2 月 22 日

3) 影响版本

用友 GRP-U8

4) 检测规则

检测流量中是否存在以下路径：

/u8qx/SmartUpload01.jsp

并同时检测上传的文件名和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快升级至最新版本，下载地址如下：https://yonyou.com/

若无法进行升级的情况下，请通过防火墙等安全设备限制访问策略，设置内容检测机制和白名单访问

如非必要，禁止公网访问该系统

VIP 平台链接：https://vip.vulbox.com/detail/17606051259798036 48?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QkdSUC1VOCUyMFNtYXJ0VXBsb2FkMDElMjAlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.9 奇安信天擎 rptsvr 任意文件上传

1) 漏洞描述

奇安信 天擎管理中心 <=V6.7.0.4130 版本的 rptsvr 接口存在任意文件上传漏洞，可上传恶意文件至服务器，执行脚本文件。

2) 爆发时间

2024 年 1 月 17 日

3) 影响版本

奇安信 天擎管理中心 <=V6.7.0.4130

4) 检测规则

检测流量中是否存在以下路径：

/rptsvr/upload

并检测上传文件名后缀和文件内容的类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

下载地址：https://hk.qianxin.com/product/detail/pid/220

VIP 平台链接：https://vip.vulbox.com/detail/1747577297541664768?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNSVBNSU4NyVFNSVBRSU4OSVFNCVCRiVBMSVFNSVBNCVBOSVFNiU5MyU4RSUyMHJwdHN2ciUyMCVFNCVCQiVCQiVFNiU4NCU4RiVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCUyMiU3RA==&origin=intellList

3.10通达 OA privateUpload 任意文件上传漏洞

1) 漏洞描述

通达 OA（Office Anywhere 网络智能办公系统）是由北京通达信科科技有限公司自主研发的协同办公自动化软件，是与中国企业管理实践相结合形成的综合管理办公平台。通达 OA 为各行业不同规模的众多用户提供信息化管理能力，包括流程审批、行政办公、日常事务、数据统计分析、即时通讯、移动办公等，帮助广大用户降低沟通和管理成本，提升生产和决策效率。

通达 OA privateUpload.php 存在前台任意文件上传漏洞，攻击者可通过该漏洞获取服务器权限。

2) 爆发时间

2023 年 12 月 19 日

3) 影响版本

通达 OA 2011

4) 检测规则

检测流量中是否存在以下路径：

/general/vmeet/privateUpload.php?fileName

同时检测上传文件的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用该产品的用户尽快联系厂商更新至安全版本。下载链接如下：https://www.tongda2000.com

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2、文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

3、文件上传目录安全性： 确保上传的文件保存在安全的目录中，并严格限制文件上传目录的权限。不要允许用户上传文件到具有执行权限的目录。

4、强化访问控制：实施严格的访问控制措施，包括强密码策略、角色权限管理和多因素身份验证，以减少未授权访问和滥用漏洞的风险。

VIP 平台链接：https://vip.vulbox.com/detail/1737025040391737344?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4MCU5QSVFOCVCRSVCRU9BJ

TIwcHJpdmF0ZVVwbG9hZCUyMCVFNCVCQiVCQiVFNiU4NCU4RiVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.11宏景 eHR OfficeServer.jsp 任意文件上传漏洞

1) 漏洞描述

宏景 eHR 人力资源管理软件是一款人力资源管理与数字化应用相融合，满足动态化、协同化、流程化、战略化需求的软件。

宏景eHR 人力资源管理软件 OfficeServer.jsp接口处存在任意文件上传漏洞，未经过身份认证的远程攻击者可利用此漏洞上传任意文件，最终可导致服务器失陷。

2) 爆发时间

2023 年 12 月 21 日

3) 影响版本

宏景 eHR

4) 检测规则

检测流量中是否存在以下路径：

/w_selfservice/oauthservlet/%2e./.%2e/system/options/customreport/OfficeServer.jsp

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快更新至最新的版本，下载链接如下：http://www.hjsoft.com.cn/#/

若无法进行升级的情况下，请使用该产品的用户进行如下操作 1、仅允许可信 ip 访问 /w_selfservice/oauthservlet/%2e./.%2e/system/options/customreport/OfficeServer.jsp 路由

VIP 平台链接：https://vip.vulbox.com/detail/1737663315695505408?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNSVBRSU4RiVFNiU5OSVBRmVIUiUyME9mZmljZVNlcnZlci5qc3AlMjAlRTQlQkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.12泛微 E-Office Init.php 任意文件上传漏洞

1) 漏洞描述

泛微 E-Office init.php 文件存在任意文件上传漏洞，攻击者可以通过该漏洞直接获取网站权限。

1、执行任意代码：攻击者可以通过上传包含恶意代码的文件，执行任意代码并控制受害者的计算机或服务器，导致数据泄露、破坏或其他恶意行为。

2、篡改或删除数据：攻击者可以上传包含恶意代码的文件，并篡改或删除服务器上的重要文件或数据。

3、钓鱼攻击：攻击者可上传 html、shtm 等文件，并写入非法博彩、赌博等恶意 SEO 页面或者写入恶意 js 文件进行钓鱼来非法获取用户信息等。

2) 爆发时间

2024 年 1 月 4 日

3) 影响版本

泛微 E-Office

4) 检测规则

检测流量中是否存在以下路径：

/E-mobile/App/init.php

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快升级至最新版本，下载地址如下：https://www.eofficeoa.com/

VIP 平台链接：https://vip.vulbox.com/detail/17427843171526942 72?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRUUtT2ZmaWNlJTIwSW5pdC5waHAlMjAlRTQlQkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.13泛微 OA E-mobile lang2sql 任意文件上传漏洞

6) 漏洞描述

泛微 OA E-mobile 是一款由上海泛微网络科技股份有限公司开发的移动办公产品，专门为手机、平板电脑等移动终端用户精心打造的移动办公产品，分浏览器版和客户端版，客户端版支持主流的移动客户端，如 iPhone、iPad、Android、Windows 等。

泛微 OA E-mobile 系统 lang2sql 接口存在任意文件上传漏洞，由于后端源码中没有对文件没有校验，导致任意文件上传。攻击者可利用该参数构造恶意数据包进行上传漏洞攻击。

7) 爆发时间

2023 年 12 月 19 日

8) 影响版本

泛微 OA E-mobile

9) 检测规则

检测流量中是否存在以下路径：

/emp/lang2sql?client

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

10) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本

官网链接：https://mobile.weaver.com.cn

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2、文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

3、文件上传目录安全性： 确保上传的文件保存在安全的目录中，并严格限制文件上传目录的权限。不要允许用户上传文件到具有执行权限的目录。

VIP 平台链接：https://vip.vulbox.com/detail/1737080858638159872?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRU9BJTIwRS1tb2JpbGUlMjBsYW5nMnNxbCUyMCVFNCVCQiVCQiVFNiU4NCU4RiVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.14用友 GRP-U8 /servlet/FileUpload 文件上传漏洞

11) 漏洞描述

用友 GRP-U8 行政事业财务管理软件是用友公司专注于国家电子政务事业，

基于云计算技术所推出的新一代产品，是我国行政事业财务领域最专业的政府财务管理软件。

用友 GRP-U8R10 中存在文件上传漏洞。未经授权的攻击者可以通过 /servlet/FileUpload 构造特殊的请求包上传恶意 Webshell 文件，进行远程代码执行，从而控制服务器。

12) 爆发时间

2023 年 12 月 5 日

13) 影响版本

用友 GRP-U8R10

14) 检测规则

检测流量中是否存在以下路径：

/servlet/FileUpload?fileName

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

15) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://security.yonyou.com/#/patchInfo?foreignKey=c7d479f24a1442b9acb909546bdfe472

VIP 平台链接：https://vip.vulbox.com/detail/1731953126199660544?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QkdSUC1VOCUyMCUyRnNlcnZsZXQlMkZGaWxlVXBsb2FkJTIwJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.15金蝶 EAS /easportal/tools/appUtil.jsp 任意文件上传/下载漏洞

1) 漏洞描述

金蝶 EAS 存在任意文件上传/下载漏洞，攻击者可以上传包含恶意代码的文件，最终执行任意代码

1、执行任意代码：攻击者可以通过上传包含恶意代码的文件，执行任意代码并控制受害者的计算机或服务器，导致数据泄露、破坏或其他恶意行为。

2、篡改或删除数据：攻击者可以上传包含恶意代码的文件，并篡改或删除服务器上的重要文件或数据。

3、钓鱼攻击：攻击者可上传 html、shtm 等文件，并写入非法博彩、赌博等恶意 SEO 页面或者写入恶意 js 文件进行钓鱼来非法获取用户信息等。

2) 爆发时间

2024 年 1 月 2 日

3) 影响版本

金蝶 EAS

4) 检测规则

检测流量中是否存在以下路径：

/easportal/tools/getenvs.jsp

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

官方下载地址：https://www.kingdee.com/

VIP 平台链接：https://vip.vulbox.com/detail/1742086503724617728?keyword=

JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4NyU5MSVFOCU5RCVCNkVBU
yUyMCUyRmVhc3BvcnRhbCUyRnRvb2xzJTJGYXBwVXRpbC5qc3AlMjAlRTQl
QkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMl
QTAlMkYlRTQlQjglOEIlRTglQkQlQkQlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q
=&origin=intellList

3.16用友 NC XbrlPersistenceServlet 反序列化漏洞

1) 漏洞描述

用友 NC 是用友网络科技股份有限公司开发的一款大型企业数字化平台。用友 NC /service/~xbrl/XbrlPersistenceServlet 反序列化漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

2) 爆发时间

2024 年 2 月 20 日

3) 影响版本

用友 NC

4) 检测规则

检测流量中是否存在以下路径：

/service/~xbrl/XbrlPersistenceServlet

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://yonyou.com/

VIP 平台链接：https://vip.vulbox.com/detail/1759839481663459328?keyword=

JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4Qk5DJTIwWGJybFBlcnNpc3RlbmNlU2VydmxldCUyMCVFNSU4RiU4RCVFNSVCQSU4RiVFNSU4OCU5NyVFNSU4QyU5NiVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.17用友 NC DownloadServlet 反序列化漏洞

1) 漏洞描述

用友 NC 是用友网络科技股份有限公司开发的一款大型企业数字化平台。用友 NC /servlet/~ic/nc.document.pub.fileSystem.servlet.DownloadServlet 反序列化漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

2) 披露时间

2024 年 2 月 21 日

3) 影响版本

用友 NC

4) 检测规则

检测流量中是否存在以下路径：

/servlet/~ic/nc.document.pub.fileSystem.servlet.DownloadServlet

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://yonyou.com/

VIP 平台链接：https://vip.vulbox.com/detail/1760138195913281536?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4Qk5DJTI

wRG93bmxvYWRTZXJ2bGV0JUU1JThGJThEJUU1JUJBJThGJUU1JTg4JTk3JUU1JThDJTk2JUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.18Atlassian Confluence 远程代码执行漏洞 (CVE-2023-22527)

6) 漏洞描述

Confluence Data Center 是一种自托管解决方案，可为组织提供各种配置选项来满足团队协作需求。Confluence Server 是一种适用于小型团队的自托管解决方案，提供了基本的协作和知识管理功能。

Atlassian Confluence Data Center & Server 存在 模板注入代码执行漏洞。攻击者可在无需登录的情况下构造恶意请求导致远程代码执行。

7) 披露时间

2024 年 1 月 16 日

8) 影响版本

Confluence Data Center and Server 8.0.x

Confluence Data Center and Server 8.1.x

Confluence Data Center and Server 8.2.x

Confluence Data Center and Server 8.3.x

Confluence Data Center and Server 8.4.x

9) 检测规则

检测流量中是否存在以下路径：

/template/aui/text-inline.vm

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

10) 修复方案

请使用此产品的用户尽快更新至安全版本

版本号：Confluence Data Center and Server >= 8.5.4

版本链接：https://www.atlassian.com/software/confluence/download

版本号：Confluence Data Center >= 8.6.0

版本链接：https://www.atlassian.com/software/confluence/download

版本号：Confluence Data Center >= 8.7.1

版本链接：https://www.atlassian.com/software/confluence/download

VIP 平台链接：https://vip.vulbox.com/detail/1747201584368062464?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkF0bGFzc2lhbiUyMENvbmZsdWVuY2UlMjAlRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTclQTAlODElRTYlQjQlOUUoQ1ZFLTIwMjMtMjI1MjcpJTIyJTdE&origin=intellList

3.19致远 OA syncConfigManager 方法存在远程代码执行漏洞

11) 漏洞描述

致远 OA 协同管理软件为企事业组织提供了一个协同办公门户和管理平台，涵盖了组织运营涉及的协作管理、审批管理、资源管理、知识管理、文化管理、公文管理等内容，支持企事业组织的信息化扩展应用。在致远 OA 攻击者可通过构造恶意请求，绕过登陆鉴权后调用 syncConfigManager 方法进行代码执行。

1、远程代码执行（RCE）：攻击者可以构造恶意的请求数据，在操作系统上执行任意代码。获取系统权限，访问敏感数据等。

2、窃取敏感数据：攻击者可以窃取服务器上的敏感数据，如用户帐户、密码、数据库内容等。可能导致隐私泄露和数据泄露。

12) 披露时间

2024 年 1 月 4 日

13) 影响版本

致远 OA

14) 检测规则

检测流量中是否存在以下路径：

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

15) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.seeyon.com

临时处理方式：建议受影响用户针对以下路径进行访问策略限制：

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager

实际利用路径有以下多种：

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&requestCompress=gzip

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&requestCompress=gzip&managerMethod=checkDB&arguments=payload

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&managerMethod=checkDB&arguments=payload

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager&managerMethod=存在多个参数均受影响&arguments=payload

VIP 平台链接：https://vip.vulbox.com/detail/1742799280873279488?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOCU4NyVCNCVFOCVCRiU5Q09BJTIwc3luY0NvbmZpZ01hbmFnZXIlMjAlRTYlOTYlQjklRTYlQjMlOTUlRTUlQUQlOTglRTUlOUMlQTglRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODEl

RTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.20泛微 E-Mobile 6.0 Client.do SQL 注入漏洞

16) 漏洞描述

泛微 E-Mobile 6.0 是一款协同办公系统，由中国的泛微科技公司开发。该系统提供手机办公应用，将企业微信重新改造，加入更多丰富实用的功能，让沟通更加便捷。

泛微 E-Mobile 6.0 存在 SQL 注入漏洞，攻击者可以通过该漏洞进行远程代码执行。

17) 披露时间

2023 年 12 月 21 日

18) 影响版本

泛微 E-Mobile 6.0

19) 检测规则

检测流量中是否存在以下路径：

/client.do

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

20) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本官网链接：https://www.weaver.com.cn/

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、访问控制：仅允许可信用户或 IP 访问/client.do

2、强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.vulbox.com/detail/17377592442514350 08?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRSUyMEUtTW9iaWxlJTIwNi4wJTIwQ2xpZW50LmRvJTIwU1FMJUU2JUIzJUE4JUU1JTg1JUE1JUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList